MAIL TO:

STATE OF UTAH
DIVISION OF PURCHASING
3150 STATE OFFICE BUILDING, CAPITOL HILL
P.O. BOX 141061
SALT LAKE CITY, UTAH 84114-1061
TELEPHONE (801) 538-3026
http://purchasing.utah.gov

Invitation to Bid

Solicitation Number: **DG4025**

Due Date: **05/04/04 at 3:00 P.M.**

Date Sent: April 9, 2004

.

Goods and services to be **MULTI-STEP BID FOR IT VULNERABILITY ASSESSMENT FOR THE DEPARTMENT OF ADMINISTRATIVE SERVICES**

Please complete

Company Name		Federal Tax Identification Number	
Ordering Address	City	State	Zip Code
Remittance Address (if different from ordering address)	City	State	Zip Code
Type ☐ Corporation ☐ Partnership ☐ Proprietorship Government	Company Contact Person		
Telephone Number (include area code)	Fax Number (include area code)		
Company's Internet Web Address	Email Address		
Discount Terms (for bid purposes, bid discounts less than 30 days will not be considered)	Days Required for Delivery After Receipt of Order (see attached for any required minimums)		

The following documents are included in this solicitation: Solicitation forms, instructions and general provisions, and specifications. Please review all documents carefully before completing.

The undersigned certifies that the goods or services offered are produced, mined, grown, manufactured, or performed in Utah. Yes_____ No_____. If no, enter where produced, etc._____

Offeror's Authorized Representative's Signature	Date
Type or Print Name	Position or Title

STATE OF UTAH
DIVISION OF PURCHASING

Invitation to Bid

Solicitation Number: DG4025

Due Date: 05/04/04

Vendor Name:

DESCRIPTION
MULTI-STEP BID FOR IT VULNERABILITY ASSESSMENT FOR THE DIVISION OF INFORMATION TECHNOLOGY SERVICES PER ATTACHED SPECIFICATIONS. THIS WILL RESULT IN A 1 YEAR CONTRACT WITH 3 (1) YEAR OPTIONS TO RENEW. QUESTIONS CONCERNING THIS MULTI-STEP BID ARE DUE IN WRITING BY 4/22/2004 AT 5:00 P.M. MOUNTAIN STANDARD TIME TO MICHAEL ALLRED AT **mwallred@utah.gov** OR VIA FAX AT 801-538-3623. QUESTIONS CONCERNING BID PROCESS CAN BE ADDRESSED TO DEBBIE GUNDERSEN AT 801-538-3150. ********** REFERENCE RX: 100 49000000028; COMMODITY CODE(S): 91828000000

INVITATION TO BID - INSTRUCTION AND GENERAL PROVISIONS

1. BID PREPARATION: (a) All prices and notations must be in ink or typewritten. (b) Price each item separately. Unit price shall be shown and a total price shall be entered for each item bid. Errors may be crossed out and corrections printed in ink or typewritten adjacent and must be initialed in ink by person signing quotation. (c) Unit price will govern, if there is an error in the extension. (d) Delivery time is critical and must be adhered to as specified. (e) Wherever in this document an item is defined by using a trade name of a manufacturer and/or model number, it is intended that the words, "or equivalent" apply. "Or equivalent" means any other brand that is equal in use, quality, economy and performance to the brand listed as determined by the Division of Purchasing & General Services (DIVISION). If the vendor lists a trade name and/or catalog number in the bid, the DIVISION will assume the item meets the specifications unless the bid clearly states it is an alternate, and describes specifically how it differs from the item specified. All bids must include complete manufacturer's descriptive literature if quoting an equivalent product. All products are to be of new, unused condition, unless otherwise requested in this solicitation. (f) By signing the bid the vendor certifies that all of the information provided is accurate, that they are willing and able to furnish the item(s) specified, and that prices quoted are correct. (g) This bid may not be withdrawn for a period of 60 days from bid due date.

2. SUBMITTING THE BID: (a) The bid must be signed in ink, sealed in a properly-addressed envelope, and either mailed or delivered to the DIVISION OF PURCHASING, 3150 State Office Building, Capitol Hill, Salt Lake City, UT 84114-1061 by the "Due Date and Time." **The "Bid Number" and "Due Date" must appear on the outside of the envelope.** (b) Bids, modifications, or corrections received after the closing time on the "Due Date" will be considered late and handled in accordance with the Utah Procurement Rules, section R33-3-109. (c) **Your bid will be considered only if it is submitted on the forms provided by the state. Facsimile transmission of bids to DIVISION will not be considered.** (d) All prices quoted must be both F.O.B. Origin per paragraph 1.(c) and F.O.B. Destination. Additional charges including but not limited to delivery, drayage, express, parcel post, packing, cartage, insurance, license fees, permits, costs of bonds, or for any other purpose must be included in the bid for consideration and approval by the DIVISION. Upon award of the contract, the shipping terms will be F.O.B. Destination, Freight Prepaid with freight charges to be added to the invoice unless otherwise specified by the DIVISION.

3. SOLICITATION AMENDMENTS: All changes to this solicitation will be made through written addendum only. Bidders are cautioned not to consider verbal modifications.

4. PROPRIETARY INFORMATION: Suppliers are required to mark any specific information contained in their bid which is not to be disclosed to the public or used for purposes other than the evaluation of the bid. Each request for nondisclosure must to be accompanied by a specific justification explaining why the information is to be protected. Pricing and service elements of any bid will not to be considered proprietary. Bids submitted may to be reviewed and evaluated by any persons at the discretion of the state.

5. SAMPLES: Samples of item(s) specified in this bid, when required by DIVISION, must to be furnished free of charge to DIVISION. Any item not destroyed by tests may, upon request made at the time the sample is furnished, to be returned at the bidder's expense.

6. WARRANTY: The contractor agrees to warrant and assume responsibility for all products (including hardware, firmware, and/or software products) that it licenses, contracts, or sells to the State of Utah under this contract for a period of one year, unless otherwise specified and mutually agreed upon elsewhere in this contract. The contractor (seller) acknowledges that all warranties granted to the buyer by the Uniform Commercial Code of the State of Utah applies to this contract. Product liability disclaimers and/or warranty disclaimers from the seller are not applicable to this contract unless otherwise specified and mutually agreed upon elsewhere in this contract. In general, the contractor warrants that: (1) the product will do what the salesperson said it would do, (2) the product will live up to all specific claims that the manufacturer makes in their advertisements, (3) the product will be suitable for the ordinary purposes for which such product is used, (4) the product will be suitable for any special purposes that the State has relied on the contractor's skill or judgement to consider when it advised the State about the product, (5) the product has been properly designed and manufactured, and (6) the product is free of significant defects or unusual problems about which the State has not been warned. Remedies available to the State include the following: The contractor will repair or replace (at no charge to the State) the product whose nonconformance is discovered and made known to the contractor in writing. If the repaired and/or replaced product proves to be inadequate, or fails of its essential purpose, the contractor will refund the full amount of any payments that have been made. Nothing in this warranty will be construed to limit any rights or remedies the State of Utah may otherwise have under this contract.

7. DIVISION APPROVAL: Purchase orders placed, or contracts written, with the state of Utah, as a result of this bid, will not to be legally binding without the written approval of the director of the DIVISION.

8. AWARD OF CONTRACT: (a) the contract will to be awarded with reasonable promptness, by written notice, to the lowest responsible bidder that meets the specifications. Consideration will to be given to the quality of the product(s) to be supplied, conformity to the specifications, the purpose for which required, delivery time required, discount terms and other criteria set forth in this invitation to bid. (b) The bids are opened publicly in the presence of one or more witnesses. the name of each bidder, and the amount of the bid is recorded. Each bid, and the record, is open to public inspection. (c) The DIVISION may accept any item or group of items, or overall low bid. the DIVISION has the right to cancel this invitation to bid at any time prior to the award of contract. (d) The DIVISION can reject any and all bids. And it can waive any informality, or technicality in any bid received, if the DIVISION believes it would serve the best interest of the State. (e) Before, or after, the award of a contract the DIVISION has the right to inspect the bidder's premises and all business records to determine the holder's ability to meet contract requirements. (f) DIVISION does not guarantee to make any purchase under awarded contract(s). Estimated quantities are for bidding purposes only, and not to be interpreted as a guarantee to purchase any amount. (g) Utah has a reciprocal preference law which will to be applied against bidders bidding products or services produced in states which discriminate against Utah products. For details see Section 63-56 20.5 -20.6, Utah Code Annotated.

9. ANTI-DISCRIMINATION ACT: The bidder agrees to abide by the provisions of the Utah Anti-discrimination Act, Title 34 Chapter 35, U.C.A. 1953, as amended, and Title VI and Title VII of the Civil Rights Act of 1964 (42 USC 2000e), which prohibit discrimination against any employee or applicant for employment, or any applicant or recipient of services, on the basis of race, religion, color, or national origin; and further agrees to abide by Executive Order No. 11246, as amended, which prohibits discrimination on the basis of sex; 45 CFR 90 which prohibits discrimination on the basis of age, and Section 504 of the Rehabilitation Act of 1973 or the Americans with Disabilities Act of 1990, which prohibits discrimination on the basis of disabilities. Also bidder agrees to abide by Utah's Executive Order, dated March 17, 1993, which prohibits sexual harassment in the workplace. Vendor must include this provision in every subcontract or purchase order relating to purchases by the State of Utah to insure that the subcontractors and vendors are bound by this provision.

10. DEBARMENT: The CONTRACTOR certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. If the CONTRACTOR cannot certify this statement, attach a written explanation for review by the STATE.

11. GOVERNING LAWS AND REGULATIONS: All state purchases are subject to the Utah Procurement Code, Title 63 Chapter 56 U.C.A. 1953, as amended, and the Procurement Regulations as adopted by the Utah State Procurement Policy Board. These are available on the Internet at www.purchasing.utah.gov

(Revision 14 Mar 2003 - IFB Instructions)

Multi-Step Bid
IT Vulnerabilities Assessment (VA)
Solicitation # DG4025

PURPOSE OF MULTI-STEP BID PROCESS

The purpose of this multi-step bid process is to enter into a contract with a qualified firm to perform a vulnerability assessment of critical information technology assets. It is anticipated that this bid may result in a contract award to a single contractor.

This document is designed to provide interested bidders with sufficient basic information to submit both a technical bid and a price bid meeting minimum requirements. Under this multi-step sealed bid procurement, price bids will be considered only in the second phase, and only from those bidders whose un-priced technical bids are found acceptable in the first phase.

SCOPE OF ASSESSMENT

The scope of this vulnerability assessment is the networks and services owned, operated, or hosted by Division of Information Technology Services. It will include a small portion of the State's Wide Area Network. It is not intended to be a full and comprehensive assessment of the entire State of Utah IT environment

BACKGROUND

The State of Utah, Department of Administrative Service, Division of Information Technology Services (ITS), is seeking a vulnerability assessment to identify vulnerabilities and obtain effective procedures to mitigate threats to critical information assets.

ISSUING OFFICE AND BID REFERENCE NUMBER

The State of Utah, Division of Purchasing, is the issuing office for this document and all subsequent addenda relating to it, on behalf of the Division of Information Technology Services. The reference number for the transaction is Solicitation # DG4025. This number must be referred to on all bids, correspondence, and documentation relating to the bid.

SUBMITTING YOUR BID

One original and four identical copies of the technical bid, and one copy of the price bid (submitted in a separate envelope marked **"Price Bid"**), must be received at the State of Utah, Division of Purchasing, 3150 State Office Building, Capitol Hill, Salt Lake City, Utah 84114, prior to the closing date and time specified. Bids received after the deadline will be late and ineligible for consideration. All items submitted must have

company name, bid number (DG4025), and technical information or price quote clearly marked on the outside of the envelope. All bids are due by May 4, 2004 at 3:00 p.m.

LENGTH OF CONTRACT

The contract resulting from this bid will be for a period of one-year. The contract may be extended beyond the original contract period year-to-year for up to three additional years at the State's discretion and by mutual agreement.

PRICE GUARANTEE PERIOD

All pricing must be guaranteed for one-year. Following the guarantee period, any request for price adjustment must be for an equal guarantee period, and must be made at least 30 days prior to the effective date. Requests for price adjustment must include sufficient documentation supporting the request. Any adjustment or amendment to the contract will not be effective unless approved by the State Director of Purchasing. The State will be given the immediate benefit of any decrease in the market, or allowable discount.

STANDARD CONTRACT TERMS AND CONDITIONS

Any contract resulting from this bid will include the State=s standard terms and conditions. These may be accessed on the Internet at:

http://www.purchasing.utah.gov/contractinfo/TermsAgency.pdf

QUESTIONS

All questions must be submitted in writing and may be submitted to Michael Allred via e-mail at: mwallred@utah.gov, or via fax at: 801-538-3623. Questions are due by 5:00 p.m. on Thursday April 22, 2004. Questions received after that date may not be answered. Answers will be given via an addendum posted on the Division of Purchasing website.

DISCUSSIONS WITH BIDDERS

A discussion between the State Purchasing agent and a bidder to clarify their technical bid may be required at the sole discretion of the State after submittal of technical bids. However, the State may award a contract based on the initial technical bid received without a discussion with the bidder. If a bidder is required to meet with the State for clarification, any expenses incurred by the bidder will be the bidder's responsibility.

PROPRIETARY INFORMATION

After award, all bids become public information. Proprietary information can be protected under limited circumstances, such as client lists and non-public financial statements. Pricing and service elements are not considered proprietary. An entire bid may not be marked as proprietary. Bidders must clearly identify specific proprietary information in the Executive Summary, and mark that information in the body of the bid. The Executive Summary must contain specific justification, explaining why the information is to be protected.

Bids may be reviewed and evaluated by any person as determined by the State. All materials submitted become the property of the State of Utah, and may or may not be returned, at the discretion of the State.

DETAILED SCOPE OF WORK

The target of this vulnerability assessment are the networks and servers owned, operated, or hosted by ITS. The purpose of this vulnerability assessment is to uncover potential security weaknesses in the State of Utah WAN core and ITS hosting environment. It will include a small portion of the State Wide Area Network (WAN). It is not intended to be a full and comprehensive assessment of the entire State of Utah IT environment.

The general activities conducted during this assessment will include:

- the use of proprietary, COTS, and/or open source tools to conduct automated scanning of known technical vulnerabilities in networked systems;
- techniques for conducting targeted testing on specific systems that may have escaped detection during automated scanning, to identify undocumented or new vulnerabilities;
- penetration testing that simulates methods used by intruders to gain unauthorized access to an organization's systems and then compromise them; and,
- to review existing State and ITS security policies and compare them to recommended industry best practices.

This assessment will include a large number of diverse systems running different levels of operating systems. Detail of the system being scanned will not be identified during the bid process for security reasons.

Phase I: Assessing Threats to Infrastructure

Discovery of Known Vulnerabilities in Applications and Operating Systems

Using active scanning tools, identify vulnerabilities that could be exploited to access the network, systems, applications, data, or devices that have a critical role in assuring the confidentiality, integrity, and availability of services.

The scan will not be limited to the well-known ports and should include all 65,535 ports.

Prior to the start of the assessment, the selected vendor will be required to provide a comprehensive list of each tool that will be used and the components and assets (systems, networks, data, personnel) it will examine.

The probable number IP addresses to be scanned and assessed is **2700.**

The analyses should include, but not be limited to, identifying and evaluating the following:

- Windows specific vulnerabilities, such as Restrict Anonymous, default sharing permissions, and IIS bugs;
- vulnerable implementations of BIND, DNS, Sendmail, SMTP, and routing protocols;
- weak default configurations and built-in default accounts;
- weak authentication methods, such as LAN Manager allowed on Windows' networks, and the use of Berkley R commands, such as rlogin on networks;
- use of clear-text services, such as Telnet, FTP, POP3, and IMAP;
- auditing to reveal poor passwords and excessive account privileges;
- discovery and review of remote control application VNC, pcAnywhere, and GotoMyPC;
- review of virus definition currency across all tested systems; and,
- an audit for common application vulnerabilities, such as:

    - Cross-site Scripting
    - SQL Injection
    - Parameter Tampering
    - Demo or Left-over Code
    - Cookie Poisoning
    - Database Server
    - Web Server
    - Buffer Overflow

Discovery of Network Vulnerabilities

- Perimeter defenses of Internet-connected systems:

    - Including border routers, firewalls, DMZ public services (Web server, FTP, external DNS, etc.).

- Network enumeration and mapping. Using publicly available information, such as whois, ARIN, and other Internet resources to footprint the network and attempt ping sweeps, trace routes, operating system identification, port scanning, zone-

transfers, and other techniques to determine how vulnerable the network is to information gathering attacks.

- Review the effectiveness of access control devices, such as firewalls and routers.
- Review the presence of unnecessary services on networked systems, particularly servers.
- Review the effectiveness of logging, monitoring, and intrusion detection.
- Discovery of weak remote administration practices for key systems, such as the absence of encryption.
- Attempt unauthorized access and use of network resources via wireless network connections.

Phase II: Determine Extent of Exposure to Identified Threats

This portion of the assessment will be done after careful consideration and with coordination of State security and operation staff. In this phase, the vendor will conduct a penetration of threats identified during Phase One's assessment to determine the level and risk of the threat.

Denial-of-service Attack

Construct a flood of SYN packets to test the infrastructure's ability to withstand a denial-of-service attack (DOS).

Phase III: Review Security Policies and Procedure Compliance

In this phase the vendor will conduct a review of the current Security policies and procedures to determine whether they:

1. Address the key factors affecting security.
2. Allow for effective compliance, implementation, and enforcement.
3. Reference or conform to established standards.
4. Provide clear and comprehensive guidance.
5. Define and communicate roles, responsibilities, authorities, and accountabilities for all individuals, organizations, and the interface with critical systems.

- Conduct a compliance audit with documented security policies.
- Conduct a policy audit identifying security best practices against existing State Policies.

Phase IV: Post-Assessment and Reporting

In this phase the vendor will prepare and submit a report of the assessment and findings of the current state of security for ITS. The vendor will prepare and submit an action plan that prioritizes assessment recommendations by relative impact; estimates mitigation costs; and, captures lessons learned and best practices.

The vendor will provide a concise and understandable vulnerability assessment report. This should include:

- an Executive Summary to be presented to the State CIO and the ITS Division management;
- technical detail, including identified vulnerabilities per devices (data should be concise and eliminate as many false positives as possible);
- a recommendation and remediation plan for identified vulnerabilities;
- an explanation of the risk of exposure, and not just the resolution;
- a prioritized and ranked list of vulnerabilities and the evaluation criteria used; and,
- a determination of the impact that the exploit might have on ITS operations.

Reporting Options

- The report must only be made available to key ITS management and personal.
- The vendor must acknowledge that the information and reports created are the property of the State of Utah and are under its control.
- Any data or reports stored by the vendor must be stored at the State or stored using 3DES or greater encrypted method and be accessible only to specific, authorized users.

Phase V: Retesting of Vulnerabilities

During this phase the State of Utah requires the capability to rerun the assessment tests on individual servers and network segments, as issues are resolved. The State must have the capability to rerun test to verify that vulnerabilities have been resolved.

TECHNICAL REQUIREMENTS AND COMPANY QUALIFICATIONS

Demonstrated Financial Stability

The vendor must be a sustainable business and have sufficient capital to continue to be a going concern. Provide your most recent audited annual report and financial statement and those of your key investors, if they are not publicly available.

The vendor must have been in the Information Security business for at least two years. Provide the number of years that your organization has been in the Information Security field.

The vendor must demonstrate that Information Security and Vulnerability Assessments are a key part of their operating revenue and that this is not a first time bid or new business direction for the vendor. Provide information on the number and percentage of staff that is involved in security services and vulnerability assessments, as well as the percentage of revenue derived from security services and vulnerability assessments.

Method for Performing Vulnerability Assessment

The vendor must have a defined method for performing vulnerability assessments. Provide a brief overview regarding your standard process for performing a vulnerability assessment. If you use a formal method, like Octave, COBRA, or other assessment method, please describe how you have implemented it in other assessments.

- Provide information on which portion of the assessment will be conducted remotely, onsite, or a combination of both.
- Provide any special requirements or access needed to conduct the assessment.
- For onsite assessment, detail required equipment and staff access needed.

Qualification and Expertise of Staff Proposed for This Project

The vendor must demonstrate that its staff has the technical expertise to do a vulnerability assessment of this size and scope. Provide a list of your employees that will participate in the assessment, and include their networking and systems experience and certifications. Also include operating systems and versions (Windows, Linux, UNIX, Solaris, NetWare, CISCO IOS).

All vendor personnel involved in the assessment must have submitted to, and successfully completed, a current background check. Provide certification that background and security checks have been conducted on each employee involved in the assessment and whether you are willing to disclose the results of these checks. The vendor may not switch or substitute staff to the project without written notification and approval of ITS.

The vendor must verify that all employees participating in the assessment have been bonded. The vendor must also include a description of the surety bond and amounts. Prior to beginning work the vendor must provide proof of the performance bond for the work specified as well as the Surety's financial and performance information.

Demonstrated Technical Capability

References and previous vulnerability assessment completed: The vendor must show that they have the capability to perform an assessment of this size and type. List at least five references with contact information and the overall scope of the assessment.

Time to deliver phases of the assessment: The vendor must estimate the time in workdays that each phase of the assessment will take. The vendor must show they comprehend the scope of the assessment and the ability of their staff, tools and techniques. The vendor must provide an estimated time to perform scans of individual equipment and network ranges. The vendor will be evaluated on reasonableness and the timeliness in which the assessment can be completed.

Technical ability of staff and tools to discover vulnerabilities:

Operating System vulnerabilities: The vendor must show that the tools and techniques they use have the ability to discover currently known vulnerabilities in the operating systems it inspects. The vendor must specifically address whether the tools have the ability to input a file identifying the IP addresses that will be scanned. The State will provide this file in a text format.

Application level vulnerabilities: The vendor must show that they have the tools and techniques to discover possible application level vulnerabilities as described in the scope of work section of the bid.

Perimeter network vulnerabilities: The vendor must show that they have the tools and techniques to discover possible perimeter network vulnerabilities as described in the scope of work section of the bid.

Wireless network vulnerabilities: The vendor must show that they have the tools and techniques to discover possible vulnerabilities in the State network introduced by wireless access points.

Penetration test and denial-of-service attacks: The vendor must show that they have the tools and techniques to do a penetration test and DOS attack when and if requested by the State Security Office team.

Review of security policy and procedures: The vendor must show that they have the tools and techniques to review security policies and conduct compliance audits

Post-assessment and reporting: The vendor must demonstrate that they have the ability to provide concise and understandable reports. This could include example reports for both the executive summary and technical detail reports.

Retesting of vulnerabilities: The vendor must demonstrate that the State will have the ability to rerun assessment tests on affected systems and networks to determine if vulnerabilities continue to exist.

Confidentially and Disclosure of Results
The information identified by the vulnerability assessment is considered sensitive and confidential to the State of Utah. The information and data identified or created during the assessment is the property of the State of Utah. Vendors are not allowed to retain or store copies for any purpose beyond this assessment. The vendor must show that they can protect the information that will be exposed during this assessment. The vendor must agree not to disclose any information found during this assessment.

- Describe polices and procedures in place to ensure the protection and confidentiality of information gathered during the assessment.
- Reports and documents gathered during the assessment will only be stored using strong encryption and have limited access capabilities.
- Accidental or intentional release of confidential information will be considered a violation of any contract and may result in legal action.
- At the conclusion of the vulnerability assessment, all applications and tools used for the assessment must be removed from all State systems. This includes Trojan Horse and backdoor programs that could be left behind for later access.
- All user IDs and passwords that were compromised must be presented to the State for elimination and/or modification.
- The vendor must be willing to certify in writing that the above actions have taken place.

TECHNICAL BID FORMAT

All technical bids must be organized and tabbed with the following headings:

1. **Bid Form**. The State Invitation to Bid form, completed and signed.

2. **Executive Summary.** The one or two page executive summary is to briefly describe the bidder's technical bid. This summary should highlight the major features of the technical bid. It must indicate any requirements that cannot be met by the bidder. The reader should be able to determine the essence of the technical bid by reading the executive summary. Proprietary information requests should be identified in this section.

3. **Detailed Response.** This section should constitute the major portion of the technical bid and must contain at least the following information:

    A. A complete narrative of the bidder's assessment of the work to be performed, the bidder's ability and approach, and the resources necessary to fulfill the

requirements. This should demonstrate the bidder's understanding of the desired overall performance expectations.

B. A specific point-by-point response, in the order listed, to each requirement in the technical bid.

TECHNICAL BID EVALUATION CRITERIA

Each area of the evaluation criteria must be addressed in detail in the technical bid. A committee will evaluate technical bids and score each criterion as either:

- Acceptable—Criterion is met.
- Potentially Acceptable—Clarification from the bidder is required to determine if the criterion is met; or evaluators believe that the bidder has the capability to meet the criterion by modifying their technical bid.
- Unacceptable—Criterion is not met, nor is the bidder capable of meeting the criteria.

TECHNICAL BID EVALUATION CRITERIA

- Demonstrated Financial Stability
- Method for Performing Vulnerability Assessment
- Qualification and Expertise of Staff Proposed for this Project
- Background Checks and Hiring Practices
- References and Previous Vulnerability Assessment Completed
- Time to Deliver Phases of the Assessment
- Operating System Vulnerabilities
- Application Level Vulnerabilities
- Perimeter Network Vulnerabilities
- Wireless Network Vulnerabilities
- Penetration Testing and DOS Attacks
- Review of Security Policy and Procedures
- Post-Assessment and Reporting
- Retesting of Vulnerabilities
- Confidentially and Disclosure of Results

BID PRICE FORMAT

The price will be evaluated independently from the technical bid. Only those firms who have been determined as “acceptable” during the technical evaluation (Step One) will proceed to the price evaluation (Step Two). Enumerate all costs on the attached Price Bid Form. The bid must list the price, broken out for each phase of assessment. The State may not have funding to do all phases of the assessment during this current fiscal year. The award will be made to the lowest bid from the firm determined to have

submitted a technically acceptable bid. The bid price should be submitted in a separate sealed envelope along with the technical bid. Mark the outside of the pricing envelope with the solicitation number and the company name.

IT VULNERABILITIES Assessment (VA) Bid #DG4025
Multi-Step Bid Technical Rating Sheet

Bidder: _____

Evaluator: _____

Date: _____

	Check One			
	Acceptable	Potentially Acceptable	Unacceptable	Evaluator Notes
Vendor Viability				
Demonstrated Financial Stability				
Method for Performing Vulnerability Assessment				
Qualification and expertise of staff proposed for this project.				
Background checks and hiring practices				
References and previous vulnerability assessment completed				
Time to deliver phases of the assessment				
Operating System Vulnerabilities				
Application Level Vulnerabilities				
Perimeter Network Vulnerabilities				
Wireless Network Vulnerabilities				
Penetration Testing and DOS Attacks				
Review of Security Policy and Procedures				
Post-Assessment and Reporting				
Retesting of Vulnerabilities				
Confidentially and Disclosure of Results				

Multi-Step Bid
IT Vulnerabilities Assessment (VA)

Solicitation # (DG4025)

PRICE BID

Bidder Name: _____

1. Provide a price for each phase of the project. The State may not have adequate funding in one fiscal year and may have to eliminate phases or spread them between fiscal years. The bid is a fixed bid price. The vendor may make changes if the State and the vendor agree that there was a change in the scope of the assessment.

2. Provide pricing by phase as described in the Scope of Work section of the bid and the number of IP address estimated to scan at 2700. Please include:

   Phase I—Assessing Threats to Infrastructure. $_____
   Estimated number of man-hours involved _____
   Price per IP address $_____

   Phase II—Determine Possibility of Exposure $_____
   Estimated number of man-hours involved_____
   Price per IP address $_____

   Phase III—Review Security Policy and Procedures $_____
   Estimated number of man-hours involved:_____

   Phase IV—Post-Assessment and Reporting $_____
   Estimated number of man-hours involved: _____

   Phase V—Retesting of Vulnerabilities $_____
   Estimated number of man-hours involved: _____

   Total Cost of All Phases $_____
   Total estimated vendor man-hours involved: _____

3. The assessment may require additional consulting time to help resolve vulnerabilities. List the name, job title, and hourly rate for any proposed consultants:

Name: _____ Title: _____ $ _____ / hour
Name: _____ Title: _____ $ _____ / hour
Name: _____ Title: _____ $ _____ / hour